CLAIMS

What is claimed is:

1. A method of controlling content usage in a personal communication device using a decryption key that is divided into a plurality of key-shares, the method comprises:

providing the personal communication device a first key-share in response to a request for content; and

verifying credit of a user of the personal communication device;

providing the personal communication device a second key-share when the credit is confirmed; and

combining the first and second key-shares with a third key share stored in the personal communication device for use in decrypting content.

2. The method as claimed in claim 1 wherein the method includes:

monitoring usage of the content with a security processor of the personal communications device; and

purging at least one of the key-shares from the personal communication device when the usage exceeds one of a set of measurement parameters stored in the personal communications device of the set.

3. The method as claimed in claim 2 further comprising receiving the request for the content from the personal communication device, the request identifying the content and the measurement parameters for the content.

4. The method as claimed in claim 1 further including:

receiving the content from a content server in a security server;

encrypting the content in the security server with the encryption key; and

providing the encrypted content from the security server to the personal communication device over a wireless communication link.

5. The method as claimed in claim 4 wherein the content server and the security server communicate over a non-secure network, and the method includes the content server adding security to the content prior to providing the content to the security server.

6. The method as claimed in claim 1 wherein the providing the first of the key-shares is performed by a security server in communication with the personal communication device.

7. The method as claimed in claim 1 wherein the third of the key-shares is stored in a subscriber identity module (SIM) associated with the user, and wherein a fourth of the key-shares is stored in the personal communication device and associated with a security processor of the personal communication device, and wherein the security processor combines the first, second, third and fourth key-shares to decrypt the encrypted content.

8. The method as claimed in claim 1 wherein the verifying credit of the user and the providing the second of the key-shares to the personal communication device are performed by a finance server in communication with the personal communication device.

9. The method as claimed in claim 1 wherein the plurality of key-shares are Blakley-Shamir key-shares.

10. The method as claimed in claim 1 wherein the content comprises either video content or music content.

11. The method as claimed in claim 1 further comprising generating a set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit, and wherein the personal communication device monitors usage of the content with respect to the measurement parameters and purges at least one

of the key-shares when the usage exceeds one of the measurement parameters of the set.

12. The method as claimed in claim 11 comprising a content server defining the set of measurement parameters based on preferences of a content provider.

13. The method as claimed in claim 11 wherein the date-limit defines an end calendar date for playing the content, the run-time limit defines a maximum amount of time for playing portions of the content, and the iteration limit defines a maximum number of times for playing the content or portions thereof.

14. The method as claimed in claim 12 wherein the measurement parameters have an authentication code associated therewith, and wherein a security processor of the personal communication device purges at least one of the key-shares when the authentication code fails to authenticate.

15. The method as claimed in claim 1 wherein the personal communication device receives the first and second of the key-shares over a wireless communication link.

16. A processing system for use in a personal communication device, the processing system comprising:

a security processor portion to combine a plurality of key-shares and decrypt content for the processing system, the security processor portion including a monitor for usage of the content constructed and arranged to purge at least one of the key-shares when the usage exceeds a measurement parameter; and

a communications processor portion to receive decrypted content from the security processor portion and providing decrypted content for playing on the personal communication device.

17. The processing system as claimed in claim 16 wherein the measurement parameters have an authentication code associated therewith and wherein the security processor portion purges at least one of the key-shares when the authentication code fails to authenticate.

18. The processing system as claimed in claim 16 wherein the security processor portion has a first of the key-shares stored therein, retrieves a second of the key-shares from a subscriber identity module inserted into the personal communication device, and receives a third of the key-shares from a finance server when a user's credit is verified for use of the content.

19. The processing system as claimed in claim 16 wherein the measurement parameters comprise at least one of a date-limit, a run-time limit, and an iteration limit, and wherein the security processor portion monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters of the set.

20. The processing system as claimed in claim 16 further comprising an applications processor portion to process applications running on the personal communication device, and wherein the security processor portion, communications processor portion and applications processor portion are part of a processor area and fabricated on an application specific integrated circuit (ASIC).

21. A personal communication device comprising:

a processor area to store first key-share therein;

a module receiving area to receive a subscriber identity module (SIM), the SIM having a second-key share stored therein; and

an RF interface to receive a third key-share and encrypted content over a wireless communication link,

wherein the processor area includes apparatus constructed and arranged to combine the first, second and third key-shares to decrypt the encrypted content and monitor playing of the decrypted content against measurement parameters.

22. A personal communication device as claimed in claim 21 wherein the measurement parameters have an authentication code associated therewith and wherein the processor area purges at least one of the key-shares when usage of the content exceeds a measurement parameter, or when the authentication code fails to authenticate.

23. A personal communication device as claimed in claim 21 wherein the processor area receives the third key-share from a finance server when a user is approved for use of the content in accordance with the measurement parameters.